REMARKS

Claims 1-22 are pending in this application, and claims 1 and 13 are amended herein. In view of the above amendments and the following remarks, reconsideration of the outstanding Office Action is respectfully requested.

Claims 1-8, 10-20, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,084,969 to Wright et al. in view of U.S. Patent No. 6,073,237 to Ellison. In addition, claims 9 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright and Ellison, in further view of the Irish Times article noted by the Examiner. However, Wright, Ellison, and the Irish Times article, taken alone or in combination, fail to disclose, teach or suggest all of the features recited in the claims.

For example, independent claim 1 recites a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of generating a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document, encrypting the original document with the session key to create an encrypted document, generating a proxy key based on a public key corresponding to the selected recipient, and transforming the encrypted document with the proxy key to create a transformed document, wherein the encrypted document remains in an encrypted state during the transformation to the transformed document.

Similarly, independent claim 13 recites a system operable to encrypt an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising a session key generation system that generates a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document, an encryption system that encrypts the original document with the session key to create an encrypted document, a proxy key generation system that generates a proxy key based on a public key corresponding to the selected recipient, and a transformation system that transforms the encrypted document with the proxy key to create a transformed document, wherein the encrypted document remains in an encrypted state during the transformation to the transformed document.

To the contrary, Wright discloses a system wherein a pager proxy server receives an encrypted message from a sending pager, *decrypts the encrypted message* using a session key generated by the sending pager, generates a new session key, *re-encrypts the message*, encrypts the new session key, and delivers the re-encrypted message to the destination pager. (Col. 5, lines 43-62). During this process, Wright explicitly states that the message must be decrypted prior to the re-encyrption, and is therefore in a de-encrypted state, even if only for a moment. This is evidenced by the fact that Wright further discloses that the proxy server generates a new session key between the decryption and re-encryption steps, thereby specifically illustrating the existence of a period of time during which the message is not encrypted. This type of system is acceptable provided a trusted "pager proxy server" is used to handle the decryption and subsequent re-encryption of the message, which is required by Wright. (Col. 3, lines 39-48). There is no suggestion whatsoever that the Wright's system enables the transformation of an encrypted document to create a transformed document, wherein the encrypted document remains in an encrypted state during the transformation to the transformed document. Accordingly, Wright fails to disclose, teach or suggest the noted features recited in independent claims 1 and 13.

In addition, Applicants respectfully traverse the Examiner's assertions on page 4 of the Office Action that no clear-text was revealed in the system of Wright because it is inherent to not reveal any clear-text document during the transformation due to security reasons and the purpose of safeguarding the document from unintended or untrustworthy persons that do not have the proper key or information, and submit that the Examiner has failed to meet the burden required by the courts to establish inherency for a 35 U.S.C. § 103(a) rejection. According to M.P.E.P. § 2112, the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of

ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

In particular, Applicants agree that it is a fundamental purpose of encryption to prevent the contents of the encrypted documents from being exposed to the untrusted persons in an un-encrypted state. As described above, Wright attempts to overcome the security risks of decrypting and re-encrypting a document by using the trusted proxy server to handle the decryption and re-ecryption of the document. In this type of traditional system wherein the decryption and re-encryption is handled in a trusted environment (i.e. the proxy server), the contents of the document are not revealed to untrusted persons, even when the document is in an un-encrypted state. However, should the trustworthyness of the proxy server ever be compromised, the contents of the document would clearly be revealed to anyone with access to the proxy server between the decryption of the document and the re-encryption of the document. Wright does nothing to address this possibility. Accordingly, despite the obvious desire to prevent exposure of the contents of an encrypted document to untrusted persons, Wright fails to teach a system wherein an encrypted document can be transformed in an untrusted environment.

However, this problem is directly addressed and overcome by the present invention because an encrypted document can be transformed to create a transformed document, and the encrypted document remains in an encrypted state during the transformation to the transformed document. One of the key features of the proxy encryption of the present invention is that the entity that performs the proxy transformation (e.g., third party, or a secretary) can be un-trusted, which is directly contrary to the trusted proxy server of Wright. Accordingly, it is very important that the proxy transformation maintains the encrypted document in an encrypted state during the transformation of the encrypted documents to a transformed document. Any system that requires that the document be decrypted and then re-encrypted in order to alter the encryption of the document to facilitate a transfer from a grantor to a grantee (such as the system of Wright) is not capable of maintaining the security of the encrypted document in an untrusted environment.

Similarly, Ellison is applied based on its disclosure of a 'wallet,' which is an electronic version of money held by a user is protected in part by a private key known only to the user. The private key is kept secret since the key is part of wallet data which is encrypted and stored in a computer. (See Col. 1, lines 20-26). In addition, the Irish Times article is applied based on its mentioning of the Cramer-Shoup method. However, Ellison and the Irish Times article fail to cure the deficiencies in Wright noted above.

None of the applied references render every feature of independent claims 1 and 13 obvious to a person of ordinary skill in the art under 35 U.S.C. § 103(a) for at least the reasons stated above. Accordingly, Applicants submit that independent claims 1 and 13 are patentably distinguishable over Wright, Ellison, and the Irish Times article, taken alone or in combination. The dependent claims are allowable by virtue of their dependency on independent claims 1 and 13, and also on their own merits.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,

Date: February 17, 2006

Stephen M. Hertzler
Registration No. 58,247

NIXON PEABODY LLP
401 9th Street, NW
Washington, DC 20004
(202) 585-8000